STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

DOUBET CONSULTING, LLC and GL2 PARTNERS, INC., individually and on behalf of others similarly situated,

Plaintiffs,

-against-

RACKSPACE TECHNOLOGY, INC.,

Defendant.

----------X

Civil Action No.:

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiffs DOUBET CONSULTING, LLC ("Doubet") and GL2 PARTNERS, INC. ("GL2") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Class Action Complaint against Defendant RACKSPACE TECHNOLOGY, INC. ("Rackspace" or "Defendant"), based upon their individual experiences and personal information, and investigation by their counsel.

INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, brings this class action suit against Defendant because of its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") and/or other proprietary and/or highly confidential data (collectively, "Sensitive Data") stored within Defendant's information network, to properly maintain its Hosted Exchange environment so as to provide continuous email service, and/or notify Plaintiffs and Class Members of outages so as to not unreasonably interfere with their access to their Sensitive Data.

2. Launched in 1998, Rackspace touts itself on its website (www.rackspace.com/about) as "multicloud solutions experts" and a leading provider of expertise and managed services across all the major public and private cloud technologies, assisting business customers in over 120

countries. Rackspace is the world's largest managed cloud provider and provides access to such cloud offerings as Amazon Web Services, Microsoft Azure, and OpenStack.

3. According to Defendant, at some point prior to 2:49 AM EST on or about December 2, 2022, Defendant discovered "an issue [that affected its Hosted Exchange Environments]."

4. According to Defendant, at approximately 2:49 AM EST, it was investigating the issues, but provided no further information to Plaintiffs and Class Members. As of that time, Defendant had allegedly already received "reports of connectivity issues" to its Exchange environments, admitting (albeit much later and insufficiently) that users "may experience an error upon accessing the Outlook Web App (Webmail) and syncing their email clients."

5. According to Defendant, over the next several hours, it continued its investigation regarding these connectivity and login issues, admitting (although much later) that users "may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client" or "a prompt [to] re-enter their password."

6. Over the course of the following day, Defendant's investigation continued, with Defendant acknowledging that these "connectivity and login issues greatly impact its clients.

7. According to statements made later on its website, Defendant recognized, and then apologized, for the "major disruption" these issues caused its clients.

8. According to statements made later that evening, Defendant again acknowledged that this "significant failure" in its environment was impacting its clients "greatly." At that time, it directed its clients' account administrators to "manually set up each individual user" on clients' accounts, actions that would require significant time and expense to those clients. During that recommended process, Defendant acknowledged that its clients would be "unable to connect to the Hosted Exchange service to sync new email or send mail using [the] Hosted Exchange." Defendant

further encouraged "admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately."

9. According to Defendant, as of December 3, 2022, at 1:57 AM EST, Defendant had determined, and later acknowledged, that the forgoing events were the result of a "security incident".

10. While Defendant claims to have discovered the disruption as early as December 2, 2022, Defendant did not inform victims of the Security Incident other than via an incident report/summary subsequently posted on its website. Indeed, Plaintiffs and Class Members were wholly unaware of the Security Incident, if at all, until their email accounts became unusable and/or they contacted Defendant directly to inquire as to the disruption.

11. Prior to the Security Incident, and in the normal course and scope of performing services for Plaintiffs and Class Members, Defendant acquired, collected and/or stored Plaintiffs' and Class Members' Sensitive Data. Therefore, at all relevant times, Defendant knew, or should have known, that Plaintiffs and Class Members would use Defendant's services to store and/or share Sensitive Data.

12. By obtaining, collecting, using, and deriving a benefit from storing and/or facilitating access to Plaintiffs' and Class Members' Sensitive Data, Defendant assumed legal and equitable duties to those individuals/businesses. These duties arise from state and federal statutes and regulations, as well as common law principles.

13. The confidential information that was compromised in the Security Incident can be used to gain unlawful access to online accounts of present and former clients, carry out identity theft, or commit other fraud and can be disseminated on the internet, available to those who broker and traffic in stolen PII and Sensitive Data .

14. The illegal access to PII and Sensitive Data of minors is particularly nefarious, as awareness of such access is typically delayed for a much longer period of time in the case of children as opposed to adults, giving perpetrators more time to use the PII and Sensitive Data for illegal purposes before detection.

15. While the sophistication of the methods employed in effectuating the Security Incident is not publicly known, it is certain that the Security Incident could have been avoided through basic security measures, encrypting, authentications, and training.

16. At all relevant times, Defendant promised and agreed in various documents to safeguard and protect Personal Identifiable Information (PII) and Sensitive Data in accordance with federal, state, and local laws, and industry standards, including the New York General Business Law, the New York SHIELD Act, and the Texas Deceptive Trade Practices – Consumer Protection Act. Defendant made these promises and agreements on their websites and other written notices.

17. Contrary to these promises, and despite the fact that the threat of a data breach or other security incident has been a well-known risk to Defendant, especially due to the valuable and sensitive nature of the data Defendant collects, stores and maintains, Defendant failed to take reasonable steps to adequately protect the PII and Sensitive Data of current and former clients. The Security Incident was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII and Sensitive Data.

18. As a result of Defendant's failure to take reasonable steps to adequately protect the PII and Sensitive Data of current and former clients, Plaintiffs' and Class Members' PII and Sensitive Data is now on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

19. Defendant's failure to implement and follow basic security procedures has resulted

in ongoing harm to Plaintiffs and Class Members, who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy, as well as disruption of their business operations, loss of hosted exchange services and permanent loss of countless e-mails and other stored data.

20. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Security Incident, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this incident.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of Members of the proposed Class exceeds 100, and diversity exists because some of the Plaintiffs and Class Members and Defendant are citizens of different states. Subject matter jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

22. This Court has personal jurisdiction over Defendant as it routinely conducts business in the State where this District is located, conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Security Incident was likely stored and/or maintained in accordance with practices emanating from this District.

23. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District, and because Plaintiff Doubet is headquartered in and does business within this District.

THE PARTIES

24. Plaintiff Doubet Consulting, LLC is a domestic limited liability company existing by virtue of the laws of the State of New York, conducting business within the State of New York and elsewhere, headquartered at 310 East 75th Street, New York, County and State of New York, and is a client of Defendant.

25. Plaintiff GL2 Partners, Inc. is a domestic for-profit corporation existing by virtue of the laws of the State of Texas, conducting business within the State of Texas and elsewhere, headquartered at 115 West 2nd Street, Suite 201, Fort Worth, County of Tarrant, State of Texas, and is a client of Defendant.

26. Defendant touts itself to the public as the "multicloud solutions experts" and a leading provider of expertise and managed services across all the major public and private cloud technologies, assisting business customers in over 120 countries. It claims to have "created the managed hosting industry". Rackspace is the world's largest managed cloud provider and provides access to such cloud offerings as Amazon Web Services, Microsoft Azure and OpenStack.

FACTUAL ALLEGATIONS

27. At all pertinent times, Plaintiffs were and are clients of Defendant Rackspace, through its employees and/or agents and/or servants and/or representatives, whose PII and other Sensitive Data were collected and stored by Defendant.

28. According to Defendant, at some point prior to 2:49 AM EST on or about December

2, 2022, Defendant discovered "an issue [that affected its Hosted Exchange Environments]."

29. According to Defendant, at approximately 2:49 AM EST, it was investigating the issues, but provided no further information to Plaintiff and Class Members. As of that time, Defendant had allegedly already received "reports of connectivity issues" to its Exchange environments, admitting (albeit much later and insufficiently) that users "may experience an error upon accessing the Outlook Web App (Webmail) and syncing their email clients."

30. According to Defendant, over the next several hours, it continued its investigation regarding these connectivity and login issues, admitting (although much later) that users "may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client" or "a prompt [to] re-enter their password."

31. Over the course of the following day, Defendant's investigation continued, with Defendant acknowledging that these "connectivity and login issues greatly impact its clients".

32. According to statements made later on its website, Defendant recognized, and then apologized, for the "major disruption" these issues caused its clients.

33. According to statements made later that evening, Defendant again acknowledged that this "significant failure" in its environment was impacting its clients "greatly." At that time, it directed its clients' account administrators to "manually set up each individual user" on clients' accounts, actions that would require significant time and expense to those clients. During that recommended process, Defendant acknowledged that its clients would be "unable to connect to the Hosted Exchange service to sync new email or send mail using [the] Hosted Exchange." Defendant further encouraged "admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately."

34. According to Defendant, as of December 3, 2022, at 1:57 AM EST, Defendant had

determined, and later acknowledged, that the forgoing events were the result of a "security incident".

35. Defendant's postings on its website regarding the Security Incident are as follow:

> **02:31 PM EST**
> **12/03/22**
> Our security and operations teams continue to work both internally and closely with outside experts to determine the full scope and impact of the issue involving our Hosted Exchange environment.
>
> Since our last update, we have assisted numerous customers to open replacement Microsoft 365 accounts so they can resume sending and receiving emails. This remains our topmost priority. Our support teams across the company continue working to assist customers in all hands-on deck effort during this time. We are working diligently to source additional resources to help our customers over the weekend. If you need assistance, please contact our support team via our usual support channels.
>
> Please continue to monitor our status page for the latest updates and FAQs:
> https://status.apps.rackspace.com/index/viewincidents?group=2.
>
> Again, thank you for your patience.
>
> **01:57 AM EST**
> **12/03/22**
> What happened?
>
> On Friday, Dec 2, 2022, we became aware of an issue impacting our Hosted Exchange environment. We proactively powered down and disconnected the Hosted Exchange environment while we triaged to understand the extent and the severity of the impact. After further analysis, we have determined that this is a security incident.
>
> The known impact is isolated to a portion of our Hosted Exchange platform. We are taking necessary actions to evaluate and protect our environments.
>
> Has my account been affected?
>
> We are working through the environment with our security teams and partners to determine the full scope and impact. We will keep customers updated as more information becomes available.

Has there been an impact to the Rackspace Email platform?

We have not experienced an impact to our Rackspace Email product line and platform.

At this time, Hosted Exchange accounts are impacted, and not Rackspace Email.

When will I be able to access my Hosted Exchange account?

We currently do not have an ETA for resolution. We are actively working with our support teams and anticipate our work may take several days. We will be providing information on this page as it becomes available, with updates at least every 12 hours.

As a result, we are encouraging admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

Is there an alternative solution?

At no cost to you, we will be providing access to Microsoft Exchange Plan 1 licenses on Microsoft 365 until further notice.

To activate, please use the below link for instructions on how to set up your account and users.

https://docs.rackspace.com/support/how-to/how-to-set-up-O365-via-your-cloud-officecontrol-panel

Please note that your account administrator will need to manually set up each individual user on your account. Once your users have been set up and all appropriate DNS records are configured, their email access will be reactivated, and they will start receiving emails and can send emails. Please note, that DNS changes take approximately 30 minutes to provision and in rare cases can take up to 24 hours.

IMPORTANT: If you utilize a hybrid Hosted environment (Rackspace Email and Exchange on a single domain) then you will be required to move all mailboxes (Rackspace Email and Exchange) to M365 for mail flow to work properly. To preserve your data, it is critical that you do not delete your original mailboxes when making this change.

I don’t know how to setup Microsoft 365. How can I get help?

Please leverage our support channels by either joining us in chat or by calling +1 (855) 348-9064. (INTL: +44 (0) 203 917 4743).

Can I access my Hosted Exchange inbox from before the service was brought offline?

If you access your Hosted Exchange inbox via a local client application on your laptop or phone (like Outlook or Mail), your local device is likely configured to store your messages. However, while the Hosted Exchange environment is down, you will be unable to connect to the Hosted Exchange service to sync new mail or send mail using Hosted Exchange.
If you regularly access your inbox via Outlook Web Access (OWA), you will not have access to Hosted Exchange via OWA while the platform is offline.

As a result, we are encouraging admins to configure and set up their user’s accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

Will I receive mail in Hosted Exchange sent to me during the time the service has been shut down?

Possibly. We intend to update further as we get more information.

As a result, we are encouraging admins to configure and set up their ser’s accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

08:19 PM EST
12/02/22
To our valued customers,

First and foremost, we appreciate your patience as we are working through the issue with your Hosted Exchange account, which we know impacted you greatly today. We experienced a significant failure in our Hosted Exchange environment. We proactively shut down the environment to avoid any further issues while we continue work to restore service. As we continue to work through the root cause of the issue, we have an alternate solution that will re-activate your ability to send and receive emails.

At no cost to you, we will be providing you access to Microsoft Exchange Plan 1 licenses on Microsoft 365 until further notice.

To activate, please use the below link for instructions on how to set up your account and users.

https://docs.rackspace.com/support/how-to/how-to-set-up-O365-via-your-cloud-officecontrol-panel

Please note that your account administrator will need to manually set up each individual user on your account. Once your users have been set up and all appropriate DNS records are configured, their email access will be reactivated, and they will start receiving emails and can send emails. Please note, that DNS changes take approximately 30 minutes to provision and in rare cases can take up to 24 hours.

IMPORTANT: If you utilize a hybrid Hosted environment (Rackspace Email and Exchange on a single domain) then you will be required to move all of your mailboxes (Rackspace Email and Exchange) to M365 in order for mail flow to work properly. To preserve your data, it is critical that you do not delete your original mailboxes when making this change.

Again, we apologize that this has been a major disruption to you, but we hope this will allow you to resume regular business as soon as possible.

Our support team is available to assist you via our usual support channels. Please reach out and continue to monitor our status page for further updates. Link to
incident:
https://status.apps.rackspace.com/index/viewincidents?group=2

Thanks again for your patience in this matter, we appreciate your business as a valued customer.

04:51 PM EST
12/02/22
To all of our valued customers, we understand the connectivity and login issues in our Cloud Office environments are greatly impacting you. We are working diligently to resolve the issue and it is currently our highest priority. Please continue to monitor our status page for the latest updates. Again, thank you for your patience, as we work to provide you a resolution soon.

04:01 PM EST

12/02/22
We are aware of an issue impacting our Hosted Exchange environments. Our Engineering teams continue to work diligently to come to a resolution. At this time we are still in the investigation phase of this incident and will update our status page as more information becomes available.

01:54 PM EST
12/02/22
We are aware of an issue impacting our Hosted Exchange environments. Our Engineering teams continue to work diligently to come to a resolution. At this time we are still in the investigation phase of this incident and will update our status page as more information becomes available.

09:38 AM EST
12/02/22
All hands are on the deck & right resources have been engaged and are actively working on the issue. All new updates will be posted here as they become available.

06:36 AM EST
12/02/22
We continue to investigate the connectivity and login issues to our Exchange environments. Users may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client, or a prompt to re-enter their password.

We will provide further information as this becomes available.

04:39 AM EST
12/02/22
We continue to investigate the connectivity issues to our Exchange environments. We will provide further updates as they become available.

04:32 AM EST
12/02/22
We continue to investigate the connectivity issues to our Exchange environments. We will provide further updates as they become available.

03:02 AM EST
12/02/22
We are investigating reports of connectivity issues to our Exchange environments. Users may experience an error upon accessing the

> Outlook Web App (Webmail) and syncing their email client(s).
>
> We will provide further updates as they become available.
>
> **02:49 AM EST**
> **12/02/22**
> We are investigating an issue that is affecting our Hosted Exchange environments. More details will be posted as they become available.

36. It was later disclosed that the Security Incident was due to a ransomware attack.

37. While Defendant claims to have discovered the disruption as early as December 2, 2022, Defendant did not inform victims of the Security Incident other than via an incident report/summary subsequently posted on its website. Indeed, Plaintiffs and Class Members were wholly unaware of the Security Incident, if at all, until their email accounts became unusable and/or they contacted Defendant directly to inquire as to the disruption.

38. Prior to the Security Incident, and in the normal course and scope of performing services for Plaintiffs and Class Members, Defendant acquired, collected and/or stored Plaintiffs' and Class Members' PII and Sensitive Data. Therefore, at all relevant times, Defendant knew, or should have known, that Plaintiffs and Class Members would use Defendant's services to store and/or share PII and Sensitive Data.

39. As part of Defendant's contracts with the current and former clients, Defendant promised to protect the PII, Sensitive Data and other data of current and former clients, in accordance with the applicable Federal, State and local statutes and regulations, emphasizing their purported commitment to protection of PII, Sensitive Data and other data on its website and elsewhere.

40. Defendant's website[1] claims:

> At Rackspace Technology Global, Inc., and its group companies including, but not limited to, Onica Group LLC, Rackspace US, Inc.,

[1] https://www.rackspace.com/information/legal/privacystatement

> Tricore Solutions, LLC, Rackspace Government Solutions, Inc. and RelationEdge, LLC, ("Rackspace Technology", "we", "us", and "our"), privacy commitments are fundamental to the way we run our business. Unless otherwise noted or governed by law, these commitments apply to everyone who has a relationship with us - including customers, partners, and website visitors. Rackspace Technology is committed to providing you with the best overall experience in all of our products and services. We strive to strike the right balance between using your data to ensure the quality of those experiences and protecting your privacy. We have assessed all aspects of our business and optimized the amount of data we collect to find just the right balance between data sharing and service.
>
> We endeavor to protect the security of your Personal Information. Rackspace Technology has implemented appropriate administrative, technical, and physical safeguards designed to prevent unauthorized access, use or disclosure. For example, we store the Personal Information you provide on computer servers with limited access that are located in controlled facilities. We will retain Personal Information collected from you where we have a justifiable business need to do so and for as long as is needed to fulfill the purposes outlined in this Privacy Notice, unless a longer retention period is required or permitted by law (such as legal, tax or accounting reasons).

41. Defendant has failed to maintain the confidentiality of PII, Sensitive Data and other data, failed to prevent cybercriminals from accessing and using PII, sensitive Data and other data, failed to avoid accidental loss, disclosure, or unauthorized access to PII, Sensitive Data and other data, failed to prevent the unauthorized disclosure of PII, Sensitive Data and other data, failed to provide security measures consistent with industry standards for the protection of PII, Sensitive Data and other data, failed to prevent interruption of service of current and former clients whose data Defendant has collected and stored, and failed to protect against the permanent loss of client data.

42. This Security Incident was foreseeable, in light of the much-publicized wave of data breaches in recent years. Since at least 2015, the Federal Bureau of Investigation ("FBI") has specifically advised private industry about the threat of "Business E-Mail Compromise" ("BEC").

The FBI calls BEC "a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide." The FBI notes that "scammers' methods are extremely sophisticated," and warns companies that "the criminals often employ malware to infiltrate company networks."[2]

43. Accordingly, Defendant knew, or should have known, given the vast amount of PII, Sensitive Data and other data it collects, manages, and maintains, that it was a target of security threats, and therefore understood the risks posed by unsecure data security practices and systems. Defendant's failure to heed warnings and to otherwise maintain adequate security practices resulted in this Security Incident.

44. Defendant, at all relevant times, had a duty to Plaintiffs and Class Members to properly secure their PII, Sensitive Data and other data, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, prevent interruption of service, protect against permanent loss of client data and promptly notify the Plaintiffs and Class Members when Defendant became aware of the potential that Plaintiffs' and Class Members' PII, Sensitive Data and other data may have been compromised.

45. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and the Class Members on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Defendant with their PII, Sensitive Data and other data by virtue of being current and former clients

[2] BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT, https://www.fbi.gov/news/stories/business-e-mail-compromise (last visited Apr. 20, 2020).

of Rackspace's personnel, and by virtue of Federal, State and local statutes and regulations. Defendant had the resources necessary to prevent the Security Incident but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

46. Defendant's duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities such as Defendant.

47. Defendants' duty to use reasonable security measures also arose under the New York SHIELD Act and the Texas Deceptive Trade Practices – Consumer Protection Act.

48. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, Protecting Personal Information: A Guide for Business.[3] Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system and have a response plan

[3] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Apr. 18, 2020).

ready in the event of a data breach. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." (17 C.F.R. § 248.201 (2013)).

49. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

50. Defendant failed to maintain reasonable data security procedures and practices.

51. Accordingly, Defendant did not comply with state and federal statutory and regulatory requirements and industry standards, as discussed above.

52. Defendant was at all times fully aware of its obligations to protect the PII, sensitive Data and other data of current and former clients. Defendant was also aware of the significant consequences that would result from its failure to do so.

53. To date, Defendant Rackspace has not offered identity monitoring to those affected by the Security Incident.

54. To date, Defendant has merely offered access to Microsoft Exchange Plan 1 licenses on Microsoft 365 to those affected by the Security Incident. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of the Security Incident and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class

Members' PII and other data, as well as for interruption of service and permanent loss of data.

55. Furthermore, Defendant's offer to Plaintiffs and Class Members squarely places the burden upon Plaintiffs and Class Members, rather than upon the Defendants, to implement this access and to investigate and protect themselves from Defendant's tortious acts resulting in the Security Breach, rather than automatically enrolling Plaintiffs and Class Members in identity monitoring services upon discovery of the breach.

56. As a result of the Security Incident and Defendant's failure to provide timely notice to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII, Sensitive Data and other data are now in the hands of unknown hackers, and Plaintiffs and Class Members now face an imminent, heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct. Further, Plaintiffs and class members have suffered a significant loss of service, as well as permanent loss of data. Accordingly, Plaintiffs and the Class Members have suffered "injury-in-fact." See *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

57. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiffs and Class Members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII, Sensitive Data and other data, the interruption of vital access to their E-mail accounts, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and to deal with governmental agencies, and loss of data.

58. Elliot Goldman, the principal of Plaintiff GL2 Partners, Inc., has already experienced significant costs of time and money due the Security Incident. Five of his E-email accounts were affected. Three accounts permanently lost all E-mails over one year old. Plaintiff

expended two days to restore the E-mails on the other two accounts after he managed to restore some E-mail service. His business was completely shut down for one week, with no E-mail access at all from December 2 to December 9, 2022. When Plaintiff contacted Defendant, he was placed on hold for up to seven hours each time before he could make any inquiries as to the status of his service. He estimates monetary damages alone at approximately $250,000.00.

59. Doubet had approximately 1.5 million e-mails stored with Defendant, as well as other data, including contact lists, calendars and scheduling information, much of which has been irretrievably lost as a result of the Security Incident. Doubet personnel have so far expended at least 300-400 hours attempting to remediate the disastrous effects of the Security Incident, including moving e-mails and other data that was retrievable to Microsoft Office 365. Doubet was totally closed for business for two and one-half weeks immediately following the Security Incident, and is still not fully operational. Doubet has still not been informed of the fate of its eight e-mail accounts with and information stored by Defendant, and the extent of the loss of data is still unknown, due to Defendant's lack of forthrightness. Doubet has suffered damages due to the above, including at least $50,000.00 in lost income alone.

CLASS ACTION ALLEGATIONS

60. Plaintiffs brings this action and seeks to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of themselves, and the following proposed Classes (collectively, the "Class").

61. The Nationwide Class is defined as follows: All individuals and business entities residing in the United States whose PII, Sensitive Data and other data was compromised and/or lost, or whose businesses were interrupted, in the Security Incident occurring on or about December 2, 2022.

62. The New York Class is defined as follows: All individuals and business entities residing in New York whose PII, Sensitive Data and other data was compromised and/or lost, or whose businesses were interrupted, in the Security Incident occurring on or about December 2, 2022.

63. The Texas Class is defined as follows: All individuals and business entities residing in Texas whose PII, Sensitive Data and other data was compromised and/or lost, or whose businesses were interrupted, in the Security Incident occurring on or about December 2, 2022.

64. Excluded from each of the above proposed Classes are: Defendant, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant; and judicial officers to whom this case is assigned and their immediate family Members.

65. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

66. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

67. Numerosity. Fed. R. Civ. P. 23(a)(1). Pursuant to Rule 23(a)(1), the Members of the Class are so numerous and geographically dispersed that the joinder of all Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, the proposed Class includes potentially hundreds of thousands of individuals whose PII, Sensitive Data and other data was compromised and/or lost, or whose businesses were interrupted, in the Security Incident. Class Members may be identified through objective means, including by and through Defendant's business records. Class Members may be notified of the pendency of this action by recognized,

Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

68. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Pursuant to Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

(a) Whether Defendant had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class Members' PII, Sensitive Data and other data, including by vendors;

(b) Whether Defendant breached its legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs' and Class Members' PII, Sensitive Data and other data;

(c) Whether Defendant's conduct, practices, actions, and omissions, resulted in or were the proximate cause of the Security Incident, resulting in the loss of PII, Sensitive Data and other data of Plaintiffs and Class Members, and the interruption of clients' E-mail access;

(d) Whether Defendant had a legal duty to provide timely and accurate notice of the Security Incident to Plaintiffs and Class Members;

(e) Whether Defendant breached its duty to provide timely and accurate notice of the Security Incident to Plaintiffs and Class Members;

(f) Whether and when Defendant knew or should have known that its computer systems were vulnerable to attack;

(g) Whether Defendant failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiffs' and Class Members' PII, Sensitive Data

and other data, and E-mail access, including by vendors;

(h) Whether Defendant breached express or implied contracts with the various and several Plaintiffs and Class Members in failing to have adequate data security measures despite promising to do so;

(i) Whether Defendant's conduct was negligent;

(j) Whether Defendant's conduct was *per se* negligent;

(k) Whether Defendant's practices, actions, and omissions constitute unfair or deceptive business practices;

(l) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of their personal and financial information, loss of E-mail access, and loss of data, and

(m) Whether Plaintiffs and Class Members are entitled to relief, including damages and equitable relief.

69. Typicality. Fed. R. Civ. P. 23(a)(3). Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Members of the Class. Plaintiffs, as all Members of the Class, were injured through Defendant's uniform misconduct described above and assert similar claims for relief. The same events and conduct that give rise to Plaintiffs' claims also give rise to the claims of every other Class Member because Plaintiffs and each Class Member are persons that have suffered harm as a direct result of the same conduct engaged in by Defendants and resulting in the Security Incident.

70. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4). Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately represent the interests of the Class Members. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class Members.

Plaintiffs' attorneys are highly experienced in the prosecution of consumer class actions and data breach cases.

71. Superiority (Fed. R. Civ. P. 23(b)(3). Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Members of the Class because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

72. Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)). In the alternative, this action may properly be maintained as a class action, because:

(a) The prosecution of separate actions by individual Members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Members of the Class, which would establish incompatible standards of conduct for Defendant; or

(b) The prosecution of separate actions by individual Members of the Class would create a risk of adjudications with respect to individual Members of the Class which would, as a practical matter, be dispositive of the interests of other Members of the Class not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

73. Issue Certification (Fed. R. Civ. P. 23(c)(4). In the alternative, the common questions

of fact and law, set forth above, are appropriate for issue certification on behalf of the proposed Class.

FIRST CAUSE OF ACTION FOR NEGLIGENCE
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

74. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

75. Defendants required Plaintiffs and Class Members to submit non-public, sensitive PII, Sensitive Data and other data as part of the provision of cloud-hosting services by Defendant Rackspace.

76. Defendant had, and continues to have, a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII, Sensitive Data and other data. Defendant also had, and continues to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the collection, storage and protection of PII, Sensitive Date and other data within their possession, custody and control and that of its vendors.

77. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and current and former clients. The special relationship arose because Plaintiffs and the Members of the Class had entrusted Defendant with their PII, Sensitive Data and other data by virtue of being clients and former clients of Defendant Rackspace. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the Class Members from a Security Incident.

78. Defendant's duties in this regard included, but were not limited to, exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII, Sensitive Data and other data in its possession; protecting Representative Plaintiffs' and Class Members' PII, Sensitive Data and other data by using reasonable and adequate security

procedures and systems that were/are compliant with industry-standard practices; implementing processes to quickly detect the Security Incident and to timely act on warnings about data breaches, and promptly notifying Plaintiffs and Class Members of any security incident, or intrusion that affected, or may have affected, their PII, Sensitive Data or other data.

79. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII, Sensitive Data and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII, Sensitive Data and other data entrusted to it, including Plaintiffs' and Class Members' PII, Sensitive Data and other data as aforesaid. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII and other data.

80. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class Members by, *inter alia*, failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII, Sensitive Data and other data of Plaintiffs and Class Members; failing to timely and accurately disclose that Plaintiffs' and Class Members' PII, Sensitive Data and other data had been improperly acquired or accessed; failing to adequately protect and safeguard the PII, Sensitive Data and other data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII, Sensitive Data and

other data; by failing to provide adequate supervision and oversight of the PII, Sensitive Data and other data with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII, Sensitive Data and other data of Plaintiffs and Class Members, misuse the PII, Sensitive Data and other data and intentionally disclose it to others without consent; failing to adequately train its employees to not store PII, Sensitive Data and other data longer than absolutely necessary; failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' PII, Sensitive Data and other data; failing to implement processes to quickly detect data breaches, security incidents, or intrusions; failing to prevent interruption of service; failing to protect against permanent data loss, and failing to encrypt Plaintiffs' and Class Members' PII, Sensitive Data and other data and monitor user behavior and activity in order to identify possible threats.

81. Defendant, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII, Sensitive Data and other data.

82. But for Defendant's negligent breach of the above-described duties owed to Plaintiffs and Class Members, their PII, Sensitive Data and other data would not have been released, disclosed, and disseminated without their authorization, their E-mail service would not have been interrupted and severely disrupted, and their data would not have been permanently lost.

83. Plaintiffs' and Class Members' PII, Sensitive Data and other data was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendant's failure to

design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII, Sensitive Data and other data.

84. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Security Incident, Plaintiffs and Class Members have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance and restoring E-mail service; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and other economic and non-economic harm.

85. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this Security Incident constitute negligence.

SECOND CAUSE OF ACTION FOR NEGLIGENCE *PER SE*
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

86. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

87. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class Members.

88. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as

interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII, Sensitive Data and other data of Plaintiffs and Class Members. The pertinent FTC publications and orders form part of the basis of Defendant's duty in this regard.

89. Defendant required, gathered, and stored personal and financial information of Plaintiffs and Class Members as part of the provision of cloud-hosting services by Defendant Rackspace.

90. Defendant violated the FTCA by failing to use reasonable measures to protect the PII, Sensitive Data and other data of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

91. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

92. The harm that occurred as a result of the Security Incident is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

93. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identify theft; from their needing to contact agencies administering government benefits; potentially defending themselves from legal action base upon fraudulent applications for government benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the Security Incident on their lives; restoring E-mail service; closely reviewing and monitoring their

accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identify theft, which may take months or years to discover and detect.

94. Defendant's violation of the FTCA constitutes negligence *per se*.

95. For the same reasons and upon the same bases, Defendants' violation of the New York General Business Law, the New York SHIELD Act, the Texas Deceptive Trade Practices – Consumer Protection Act and various other State and local statutes, constitutes negligence *per se*.

THIRD CAUSE OF ACTION FOR BREACH OF CONTRACT
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

96. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

97. Defendant required, gathered, and stored PII, Sensitive Data and other data of Plaintiffs and Class Members as part of the provision of cloud-hosting services by Defendant Rackspace.

98. There was offer, acceptance and consideration, the consideration being the fees paid by Plaintiffs and Class Members for Defendant's services, including the provisions of those agreements pertaining to the protection of current and former clients' PII, Sensitive Data and other data.

99. The Plaintiffs and Class Members have performed and satisfied all their obligations to Defendant pursuant to their contracts.

100. Defendant breached its contractual obligations to protect the current and former clients' PII, Sensitive Data and other data it possessed and with which it was entrusted when the information was accessed by unauthorized persons as part of the Security Incident.

101. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identify theft; from their needing to contact government agencies; potentially defending themselves from legal action base upon fraudulent applications for benefits made in their names; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives; restoring E-mail service; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identity theft, which may take months or years to discover and detect.

102. The above constitutes breach of contract by Defendant.

FOURTH CAUSE OF ACTION FOR BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

103. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

104. Defendant required, gathered, and stored PII, Sensitive Data and other data of Plaintiffs and Class Members as part of the provision of cloud-hosting services by Defendant Rackspace.

105. By virtue of the above, Defendant entered into implied contracts with Plaintiffs and Class Members by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached, compromised, or stolen.

106. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

107. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect current and former clients' PII, Sensitive Data and other data, and by failing to provide timely and accurate notice to them that PII, Sensitive Data and other data was compromised as a result of the Security Incident.

108. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identify theft; from their needing to contact agencies administering government benefits; potentially defending themselves from legal action base upon fraudulent applications for government benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; restoring E-mail services; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identify theft, which may take months or years to discover and detect.

109. The above constitutes breach of implied contract by Defendant.

FIFTH CAUSE OF ACTION FOR MISREPRESENTATION
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

110. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

111. A special, privity-like relationship existed between Defendant and Plaintiffs and Class Members herein because Plaintiffs and the Class Members entrusted Defendant with their PII and other data by virtue of being current and former clients of Defendant Rackspace, with whom

Defendant had contracted to provide services, and by virtue of Federal, State and local statutes and regulations.

112. The Defendant incorrectly represented to Plaintiffs and Class Members that they would take appropriate measures to safeguard their PII, Sensitive Data and other data and promptly notify them of a data breach or Security Incident.

113. Plaintiffs and Class Members reasonably relied upon said representations in that they held Defendant in a position of trust as guardians of their PII, Sensitive Data and other data.

114. As a direct and proximate result of Defendant's misrepresentations, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identify theft; from their needing to contact agencies administering government benefits; potentially defending themselves from legal action base upon fraudulent applications for government benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; restoring E-mail service; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identify theft, which may take months or years to discover and detect.

115. The above constitutes misrepresentation on the part of Defendant.

SIXTH CAUSE OF ACTION FOR BREACH OF FIDUCIARY DUTY
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

116. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

117. A fiduciary relationship existed between Plaintiffs and Class Members and Defendant, in that Defendant was in a position of trust with respect to Plaintiffs and Class Members by virtue of being current and former clients of Defendant Rackspace, who had contracted to provide cloud-hosting services, and by virtue of Federal, State and local statutes and regulations.

118. Defendant owed a duty to Plaintiffs and Class Members to ensure that the PII, Sensitive Data and other data entrusted to it was safeguarded pursuant to common law and statute.

119. The Defendant engaged in misconduct, consisting of the failure to safeguard the PII, Sensitive Data and other data of Plaintiffs and Class Members that had been entrusted to it, in violation of the duty to exercise due care, its contractual obligations and its statutory obligations pursuant to the Federal Trade Commission Act ("FTCA"), the New York General Business Law, the New York SHIELD Act, the Texas Deceptive Trade Practices – Consumer Protection Act, and various other State and local statutes, which constitutes negligence *per se*.

120. Defendant breached the fiduciary duty that it owed to Plaintiffs and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiffs and Class Members.

121. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identify theft; from their needing to contact agencies administering government benefits; potentially defending themselves from legal action base upon fraudulent applications for government benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; restoring E-mail service; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit

alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identify theft, which may take months or years to discover and detect.

122. The above constitutes breach of fiduciary duty on the part of Defendant.

SEVENTH CAUSE OF ACTION FOR DECLARATORY JUDGMENT
(on behalf of Plaintiffs, the Nationwide Class and the New York and Texas Classes)

123. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

124. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

125. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII, Sensitive Data and other data and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII, Sensitive Data and other data. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PII, Sensitive Data and other data and remain at imminent risk that further compromises of their PII, Sensitive Data and other data will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

126. Plaintiffs and Class Members have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiffs' and Class Members' PII, Sensitive Data and other data, including Social Security numbers, while

storing it in an Internet-accessible environment and (ii) Defendants' failure to delete PII, Sensitive Data and other data they have no reasonable need to maintain in an Internet-accessible environment.

127. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII, Sensitive Data and other data of past and current clients of Defendant and its affiliates;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII, Sensitive Data and other data; and

c. Defendant's ongoing breaches of their legal duty continue to cause Plaintiffs and Class Members harm.

128. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII, Sensitive Data and other data. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test their systems for security vulnerabilities, consistent with industry standards, and

d. implement an education and training program for appropriate employees regarding cybersecurity.

129. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

130. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

131. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

EIGHTH CAUSE OF ACTION FOR VIOLATION OF NEW YORK GENERAL BUSINESS LAW §349
(on behalf of Plaintiff Doubet and the New York Class)

132. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

133. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

(a) Defendant misrepresented material facts to Plaintiff Doubet and New York Class Members

by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Doubet's and New York Class Members' PII, Sensitive Data and other data from unauthorized disclosure, release, data breaches, theft, data loss and loss of service;

(b) Defendant misrepresented material facts to Plaintiff Doubet and New York Class Members by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff Doubet's and New York Class Members' PII, Sensitive Data and other data;

(c) Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Plaintiff Doubet's and New York Class Members' PII, Sensitive Data and other data;

(d) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff Doubet's and New York Class Members' PII, Sensitive Data and other data, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

(e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Security Incident to Plaintiff Doubet and New York Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law §§ 899-aa(2) and 899-bb (SHIELD Act).

134. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff Doubet and New York Class Members) regarding the security of its network and aggregation of PII, Sensitive Data and other data.

135. The misrepresentations upon which consumers (including Plaintiff Doubet and New York Class Members) relied were material misrepresentations (*e.g.*, as to Defendant's adequate protection of PII, Sensitive Data and other data), and consumers (including Plaintiff Doubet and New York Class Members) relied on those representations to their detriment.

136. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff Doubet and other New York Class Members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability of their PII, Sensitive Data and other data.

137. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff Doubet's and New York Class Members' PII, Sensitive Data and other data were disclosed to third parties without authorization, causing and will continue to cause Plaintiff Doubet and New York Class Members damages.

138. As a direct and proximate result of Defendant's violation of NY GBL §349, Plaintiff Doubet and New York Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for government benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; interruption of business with attendant economic loss; permanent loss of data; emotional distress, and damages from identify theft, which may take months

or years to discover and detect.

139. Plaintiff Doubet and New York Class Members seek all monetary and non-monetary relief allowed by law, injunctive relief, and reasonable attorneys' fees and costs.

140. The above constitutes violation of NY GBL §349.

NINTH CAUSE OF ACTION FOR VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT
(Texas Bus. & Com. Code §§ 17.41, *et seq.*)
(on behalf of Plaintiff GL2 and the Texas Class)

141. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in the preceding paragraphs above as if set forth in full herein.

142. Plaintiff GL2 brings this claim under the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), which makes it unlawful to commit "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce." Tex. Bus. & Com. Code § 17.46.

143. Defendant is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

144. Plaintiff GL2 and the Texas Class Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

145. Defendant advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

146. Defendant engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; advertising goods or services with intent not to sell them as advertised; failing to implement and maintain reasonable security and privacy measures to protect Plaintiff GL2 and Texas Class

Members' PII, Sensitive Data and other data, which was a direct and proximate cause of the Security Incident; failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Security Incident; failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff GL2's and Texas Class Members' PII, Sensitive Data and other data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Security Incident; misrepresenting that it would protect the privacy and confidentiality of Plaintiff GL2's and Texas Subclass Members' PII, Sensitive Data and other data, including by implementing and maintaining reasonable security measures; misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff GL2's and Texas Class Members' PII, Sensitive Data and other data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq*., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052; omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff GL2's and Texas Class Members' PII, Sensitive Data and other data, and omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff GL2's and Texas Class Members' PII, Sensitive Data and other data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

147. Defendant intended to mislead Plaintiff GL2 and Texas Class Members and induce

them to rely on its misrepresentations and omissions.

148. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data/network security and ability to protect the confidentiality of consumers' PII, Sensitive Data and other data.

149. Had Defendant disclosed to Plaintiff GL2 and Texas Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a responsible company that could be trusted with valuable PII, Sensitive Data and other data regarding thousands of consumers, including Plaintiff GL2 and the Texas Class members. Defendant accepted the responsibility of being a steward of that PII, Sensitive Data and other data, while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as such, Plaintiff GL2 and the Texas Class Members acted reasonably in relying upon Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

150. Defendant had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII, Sensitive Data and other data in its possession, and the generally accepted professional standards in its industry.

151. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendant engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

152. Consumers, including Plaintiff GL2 and Texas Class Members, lacked knowledge about deficiencies in Defendant's data security because this information was known exclusively by

Defendant. Consumers also lacked the ability, experience, or capacity to secure the PII, Sensitive Data and other data in Defendant's possession or to fully protect their interests with regard to their data. Plaintiff GL2 and Texas Class Members lack expertise in information security matters and do not have access to Defendant's systems in order to evaluate its security controls. Defendant took advantage of its special skill and access to PII, Sensitive Data and other to hide its inability to protect the security and confidentiality of Plaintiff GL2 's and Texas Class Members' PII, Sensitive Data and other data.

153. Defendant intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Security Incident, which resulted from Defendant's unconscionable business acts and practices, exposed Plaintiff GL2 and Texas Class Members to a wholly unwarranted risk to the safety of their PII, Sensitive Data and other data and the security of their identities, financial information or PII, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff GL2 and Texas Class Members cannot mitigate this unfairness because they cannot undo the Security Incident.

154. Defendant acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff GL2's and Texas Class Members' rights.

155. As a direct and proximate result of Defendant's unconscionable and deceptive acts or practices, Plaintiff GL2 and Texas Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including those emanating from fraud and identity theft, time and expenses related to monitoring

their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Data. Defendant's unconscionable and deceptive acts or practices were a producing cause of Plaintiff GL2's and Texas Class Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish, interruption of business with attendant economic loss, and permanent loss of data.

156. Defendant's violations present a continuing risk to Plaintiff GL2's and Texas Class Members, as well as to the general public.

157. Plaintiff GL2 and the Texas Class Members seek all monetary and nonmonetary relief allowed by law, including economic damages, damages for mental anguish, treble damages for each act committed intentionally or knowingly, court costs, reasonably and necessary attorneys' fees, injunctive relief and any other relief which the Court deems proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Members of the Classes defined above, respectfully request that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class representative, and appoint the undersigned as Class counsel;

B. Order appropriate relief to Plaintiffs and the Classes;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiffs and the Classes pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

F. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: Brooklyn, New York
January 20, 2023

Respectfully submitted,

HELD & HINES, L.L.P.
Attorneys for Plaintiffs and the Class
2004 Ralph Avenue
Brooklyn, New York 11234
(718) 531-9700

/s/ Marc Held
Marc J. Held, Esq.
mheld@heldhines.com

/s/ Philip Hines
Philip M. Hines, Esq.
phines@heldhines.com